TOP 5 TECH MISTAKES LAWYERS MAKE AND HOW TO AVOID THEM

Data is an important asset for lawyers, and many legal firms need technology and online information access. Yet while your fine legal minds know the law inside out, your firm remains at risk of cybercriminal attack. This ebook discusses five top tech mistakes lawyers make and how to avoid them.

Law firms guard a wealth of confidential and valuable information. Hackers targeting a law firm can access personal and proprietary data, or exploit financial accounts, so it’s no surprise that cyberattacks in the legal industry are on the rise. Law firms of all sizes face many different attack types including:

- business email compromise;
- denial-of-service;
- phishing;
- data exfiltration;
- ransomware.

Any of these could lead to lost billable hours and a damaged brand reputation. There's also the cost of repair consulting, or new software and hardware. The firm might even face legal malpractice claims.

The vast majority of lawyers are well aware of the risk. They have read industry and regulatory advice, and they know to protect document management systems or improve cloud service security. Still, they continue to make common tech mistakes. We’ll discuss the top five concerns and provide strategies to mitigate risk.

#1 Failing to Encrypt Mobile Devices

Many lawyers can't function without mobile devices. They need to keep up with cases while away from the office meeting with clients or appearing in court. Now, because of the pandemic, even the most traditional lawyer has gone digital. (Even appearing in court with cat filters on their faces – oops!).

If these devices aren't encrypted, data is in danger of exposure. A stolen or lost laptop or smartphone offers access to documents and correspondence when unencrypted.

When a lawyer travels, customs can seize phones. An ill-intentioned actor could quickly copy an unencrypted device's contents before handing it back.

Strategies for Success

First, encrypt all mobile devices individual firm employees use. This will help protect data and system security in the event of theft or loss.

#2 Trusting Too Much

Between contracts and supporting evidence, expect email attachments at law firms. You tell your people to be wary of trusting attachments, but they are still going to download them. One wrong click can cause a nightmare, though.

A Canadian law firm lost six figures after hackers accessed a bookkeeper's computer. The attack likely originated from an email attachment claiming to be a free screensaver.

Trusting third-party vendors can be a problem, too. In May 2020, a UK software company left sensitive data of 193 law firms unprotected, using online legal forms that had confidential data left accessible to anyone with a browser and internet connection. The data included hashed passwords, confidential documents, passport numbers, and eye colors. The only comfort? The bad actor would have to have known where to look.

Strategies for Success

Besides educating employees about questioning attachments, IT could filter downloadable content.

Also, put in place two-factor authentication (2FA). Even the best among us pick easy passwords or reveal info on social media that informs access credentials. Installing 2FA makes it more difficult for the cybercriminal to gain access to your network. They need not only an individual's username and password but also access to the physical device where authentication is sent.

#3 Using Autocomplete in Emails

At a law firm, every minute counts. With many cases at different stages, convenient shortcuts appeal, but using the autocomplete function in Outlook or Gmail is a no-no. The email is trying to make life easier by suggesting addresses when you begin to type. Unfortunately, they don't always serve up the right address, and it's easy to miss that when you're head-down looking at the keys as you're typing type or writing an email to many people.

One drug company lawyer meant to send information to a colleague, Brad Berenson. Instead, he sent it to Alex Berenson. Alex was a New York Times reporter who now had a front-page news story in his inbox.

Strategies for Success

Don’t trust the email disclaimer about “information which may be confidential, subject to privilege, or exempt from disclosure under applicable law.”

Instead, avoid inadvertent email snafus by disabling the Reply All function. Train everyone to take a second look at the recipient line before pressing send. In especially sensitive cases, consider adding encryption to those outgoing messages.

#4 Insufficient Network Protection

Law firms are a juicy target. Discovery documents can be used for blackmail. Contracts could tip off insider trading. Intellectual property information could fuel a product war.

The law firm that relies solely on a firewall is not doing enough. Protecting the desktop computers sitting in your office environment is insufficient, especially with COVID-19 sending so many people home to work remotely. You need to protect all entry points to your network.

Strategies for Success

Install comprehensive protection at the edge of your network, too. Boost the security procedures for your remote-working solutions with 2FA.

Use remote monitoring to ensure all off-site devices get the latest software and antivirus updates.

Implement least-access policies to limit access to network resources. This means the temp, for instance, would not get the same access to your systems as the CEO. Instead, IT would customize user access to match the individual's roles and responsibilities, as giving access only to what is needed can minimize the damage if one person's account is exploited.

#5 Handling Your Own Tech Problems

You survived law school. You're smart and probably enjoy the challenge of figuring things out for yourself. But is figuring out how to authenticate your remote desktop protocol a good use of your time?

Another problem with handling your own tech, is that you're limited by what you don't know. You may miss out on areas of digital transformation that could make a big difference at your firm. Your clients will expect online payment and digital signatures, and they will want to upload supporting files to case management software in the cloud. Doing the research on the best solution for each of these is time consuming.

Your billable hours are valuable. Stick to what you know best: build new client relationships and grow your business. There's no need to start up that steep IT learning curve when help is easily available.

Strategies for Success

One option is to take a break-fix approach to technology. You recognize you can't solve every problem, and when something goes wrong you turn to the experts to come in and save the day. But this leaves you at the mercy of their schedules, and they don't know anything about what is unique to your firm's computer systems and your IT needs.

Instead, partner with a managed service provider (MSP). You'll get an IT team dedicated to your firm. They'll get to know how you're doing business, what technology you have now, and what your goals are. They'll also suggest ways to streamline processes and modernize technology, plus, you'll have someone on hand to monitor mobile devices, update software, and react quickly if something does go wrong.

CONCLUSION

You wouldn’t go into the courtroom and wing it. Exercise that same caution and care with your technology – work with an MSP. Keep operating systems and antivirus software current, limit and authenticate access, and know someone is looking out for cybersecurity threats. An MSP can also put encryption in place and create a reliable backup of your data. While you help your clients, your MSP can help you.

Phone: 01228 576090 or 01228 217100

Email: mailto:support@cumbriacomputerrepairs.co.uk

Web: http://www.cumbriacomputerrepairs.co.uk

Facebook: http://www.facebook.com/CumbriaComputerRepairs/

LinkedIn: http://www.linkedin.com/in/cumbriapcrepair/

Twitter: twitter.com/cumbriapcr